Prepared Testimony and Statement for the Record of

Joseph Pasqua
Vice President of Research
Symantec Corporation

Hearing on

Online Privacy, Social Networking, and Crime Victimization

Before the

House Judiciary Committee
Subcommittee on Crime, Terrorism, and Homeland Security

July 28, 2010
2141 Rayburn House Office Building

Mr. Chairman, Ranking Member Gohmert, and members of the Subcommittee, I am Joe Pasqua, Vice President of Research for Symantec Corporation[1]. I'm responsible for all activities within Symantec Research Labs, the company`s global research organization. Thank you for the opportunity to appear before you today to discuss the Committee's efforts to help ensure that consumers and businesses better understand the risks of social networking websites and the steps that one can take to reduce these risks before participating on such sites.

As the global information security industry leader, security is our top priority at Symantec. We are committed to assuring the security, availability and integrity of our customers' information. We protect more people from more online threats than anyone in the world. Our best-in-class Global Intelligence Network[2] allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

Symantec strives to help educate Internet users about their exposure to online risks, and to offer advice and solutions for how they can help to keep themselves and their family and friends safe online. We welcome the opportunity to provide comments as the Committee continues its important efforts to deter social network crime victimization and further enhance cybercrime law enforcement efforts. In my testimony today, I will provide the Committee with:

- Symantec's assessment of the latest social networking cybercrime threats;
- Our Insights into the inherent privacy risks associated with social networking;
- Recommended pre-cautions for consumers and businesses alike to follow to in order to avoid being victimized by cybercriminals on social network sites; and
- Issues for the Committee to consider in order to help prevent social network cybercrime.

Social network tools have changed our personal and professional lives. Consumers and businesses alike have taken to the Internet as a medium for our most personal and sensitive activities, as search engines, social networking sites, online banking, and medical information. Web sites are becoming part of the daily lives of Americans. Social networking is everywhere. It is common to find parents, children, coworkers and even the elderly on the networks across the social media world on sites such as Twitter, MySpace, Facebook, YouTube and LinkedIn.

With social networks people across the world have access to tools and options that were previously non-existent. However, there are just as many new opportunities to connect as there are to get into potential danger. Social networking has opened up many new doorways for cyber-crime, and with all the people on social networks who are completely new to technology, it is more important than ever to educate people so they are aware of these risks.

[1] Symantec is a global leader in providing security; storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

[2] Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify, analyze, deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. More than 240,000 sensors in 200+ countries monitor attack activity through a combination of Symantec products and services as well as additional third-party data sources.

The number of online U.S. households using social networks such as Facebook and MySpace has nearly doubled in the past year expanding online opportunities for criminals. The underground economy has also discovered that social networking pays. Cybercriminals have long been using the idea of these participation networks for their own purposes. The infiltration of communities, the spreading of spam or malware have in the meantime become a part of everyday life within social networks. And that trend is increasing! The potential abuses the criminals have conceived are highly varied and range from targeted spying on personal data, through spam and phishing mail distribution up to exploitation of security holes within the particular social networking platform.

Beginning in 2009, attacks against both social networking sites themselves and the users of those sites have now become standard practice for criminals. The latter half of 2009 saw attacks utilizing social networking sites increase in both frequency and sophistication. Such sites combine two factors that make for an ideal target for online criminal activity: a massive number of users and a high-level of trust among those users.

Social Networks Are a Rich Repository of Personal Information

The popularity of Facebook and other social networking sites has given hackers new ways to steal both money and information. Social networks provide a rich repository of information cybercriminals can use to refine their phishing attacks. Many Internet users are too often blasé about the information they post on the web. According to a 2009 Symantec survey, computer users under 25 years old are especially exhibiting a casual attitude to internet security with two thirds saying they aren't worried about the information they leave behind.

Nearly two thirds of computer users under 25 years old have uploaded personal photographs and private details to a social networking site. In addition, 79 percent of respondents revealed postcodes and 48 percent disclosed phone numbers on social networking sites; one in 10 has put their bank details online and one in 20 has uploaded their passport number. By comparison older internet users are more cautious about the information that they post online: under a third of 36-45 year-olds share photographs, and only two in 10 people over 46 years old share their photographs online.

People of all ages should be wary of the information that they are posting online. In a rush to embrace the advantages of sharing information on the internet, many young people have created online databanks or "tattoos" that much like a real life tattoo are difficult to remove. A "digital tattoo" is created by all the personal information web users post online and can easily be found through search engines by a potential or current employer, friends and acquaintances, or anyone who has malicious intent. Posting personal information online can also leave you vulnerable to identity theft. Details such as postcodes, birth dates or mother's maiden names can all be used by cybercriminals to crack passwords and hijack accounts to send out spam or malware to contact lists for financial gain.

Personal Data Targeted

Alongside the direct insertion of malware or the distribution of mass mailings, the cyber criminals use social networks to lure users to primed websites where they can steal personal data so that they can sell it for a profit. Targeted by the offenders are login data and classical account data, telephone numbers, email addresses and dates of birth. There's been a marked increase in "crimeware," or software used to conduct cybercrime on social networks and elsewhere. These tools fuel the black market including, botnets, keystroke loggers, spyware, backdoors, and Trojans. In 2009, Symantec created over 2.5 million new virus signatures and discovered more than 210 million distinct malware variants, a 56 percent and 75 percent increase, respectively, over the same period in 2008[3]. To put this in prospective, Symantec created more signatures in the past 15 months than in the past 18 years combined.

According to Symantec's *Report on the Underground Economy,*[4] there continues to be a well-organized underground economy specializing in the sale of stolen confidential data, particularly credit card and bank account credentials. Today's cybercriminals thrive on obtaining unauthorized information from consumers and businesses. This active underground economy has matured into an efficient, global marketplace in which stolen goods and fraud-related services are regularly bought and sold. The underground economy is geographically diverse and generates revenue for cybercriminals who range from loose collections of individuals to organized and sophisticated groups. The geographical locations of underground economy servers constantly change to evade detection by law enforcement.

Symantec has calculated that the potential worth of all credit cards advertised in the Underground Economy at $5.3 billion. The second most common category of goods and services advertised was financial accounts at 20 percent of the total. While stolen bank account information sells for between $10 and $1,000, the average advertised stolen bank account balance is nearly $40,000. The total worth of the bank accounts advertised during this reporting period was $1.7 billion.

In addition, cybercrime attack toolkits have lowered the bar to entry for new cybercriminals, making it easy for unskilled attackers to compromise computers and steal information. One such toolkit called Zues, which can be purchased for as little as $700, automates the process of creating customized malware capable of stealing personal information. Using kits like Zeus, attackers created literally millions of new malicious code variants in an effort to evade detection by security software.

Social Engineering as the Primary Attack Vector

Attackers are now going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent. Social engineering's popularity is at least in part spurred by the fact that what operating system and Web browser rests on a user's computer is largely irrelevant, as it is the actual user being targeted, not necessarily vulnerabilities on the machine. Social engineering is already one of the primary attack vectors used today, and Symantec estimates that the number of attempted attacks using social engineering techniques is continuing to increase in 2010.

If the social network sites are paying attention, and to their credit they usually are, most threats can be squashed pretty quickly. It's not targeted attacks you should be worried about, but *adapted* attacks. Adapted attacks occur when the bad guys take existing threats and use social networks to increase the effectiveness of the social engineering aspect of the attack. There is nothing like being surrounded by friends to get you to lower you guard.

[3] Symantec's Internet Security Threat Report, Volume XV, April 2010. The Symantec Internet Security Threat Report provides an annual overview and detailed analysis of Internet threat activity, malicious code, and known vulnerabilities. The report also discusses trends in phishing, spam and observed activities on underground economy servers.

[4] Symantec's Report on the Underground Economy is a survey of cybercrime activity in the underground economy. It includes a discussion of some of the more notable groups involved, as well as an examination of some of the major advertisers and the most popular goods and services available. It also includes an overview of the servers and channels that have been identified as hosts for trading, and a snapshot of software piracy using a file-sharing protocol in the public domain. This report is meant to be an analysis of certain aspects of the underground economy and is not meant to encompass a survey of Internet cybercrime as a whole. For the underground economy servers observed by Symantec, the period of observation was between July 1, 2007, and June 30, 2008.

Take the problem we are getting a lot of reports on currently—it's an advanced payment scam. This is often called a Nigerian 419 scam. But, instead of some prince in Nigeria, the scammer appears to be a friend of yours. And, instead of getting a long letter, you're contacted via a social network. What remains the same is that they both want your cash. You'll undoubtedly see endless variations on this theme, but the basic scam is that someone you are connected to via a social network posts a status message or instant messages you, or sends you an email stating that they are in trouble. They are apparently stuck somewhere -- London is currently popular -- and have gotten lost or been robbed of all their cash or both. They need you to "loan" them some money so they can get home.

Unlike helping the Prince of Nigeria, your motivation to send the cash is noble; you want to help out a friend. But, here's the thing. Whoever is contacting you is an imposter. The imposter has broken into your friend's account and having unrestricted access to all of that personal information makes it pretty easy to make convincing claims. With a stolen login and password, someone can be very convincing while pretending to be your friend.

The Proliferation of Rogue Security Software

A growing cybercrime trend is the use of misleading software programs or commonly known as RogueAV programs. Symantec's *Report on Rogue Security Software*[5], based on data obtained during the 12-month period of July 2008 to June 2009, reveals that cybercriminals are now employing increasingly persuasive online scare tactics to convince users to purchase rogue security software. Rogue security software, or "scareware," is software that pretends to be legitimate security software. These rogue applications provide little or no value and may even install malicious code or reduce the overall security of the computer.

To encourage unsuspecting users to install their rogue software, cybercriminals place deceptive website ads that prey on users' fears of security threats. These ads appear credible but typically include false claims such as "If this ad is flashing, your computer may be at risk or infected," urging the user to follow a link to scan their computer or get software to remove the threat. According to the study, 93 percent of the software installations for the top 50 rogue security software scams were intentionally downloaded by the user. As of June 2009, Symantec detected over 250 distinct rogue security software programs and had received reports of 43 million rogue security software installation attempts. Symantec blocked 4.8 million attacks of just one version of this type of malware.

Targeted Attacks on Companies

Given the potential for monetary gain from compromised corporate intellectual property (IP), cybercriminals have turned their attention toward enterprises. Symantec's Internet Security Threat Report found that attackers are leveraging the abundance of personal information openly available on social networking sites to synthesize socially engineered attacks on key individuals within targeted companies.

The information, which members of social networks divulge about themselves and their living circumstances, also permits cyber criminals to carry out targeted attacks on companies. With the information that you can collect in Xing about a particular company, targeted phishing mails can be sent to company management, sales

[5] The Symantec Report on Rogue Security Software, developed by the company's Security Technology and Response (STAR) organization, is an in-depth analysis of rogue security software programs. The report includes an overview of how these programs work and how they affect users, including their risk implications, various distribution methods, and innovative attack vectors. It includes a brief discussion of some of the more noteworthy scams as well as an analysis of the prevalence of rogue security software globally. It also includes a discussion on a number of servers that Symantec observed hosting these misleading applications. Except where otherwise noted, the period of observation for this report was from July 1, 2008 to June 30, 2009.

or accounts. This can take into account, position within the company, colleagues and hobbies. Tailor-made spyware Trojans infiltrated in this manner can ruin companies.

A Facebook message sent last fall between co-workers at a large U.S. financial firm which read: "Hey Alice, look at the pics I took of us last weekend at the picnic. Bob". The social network message rang true enough. Alice had, in fact, attended a picnic with Bob, who mentioned the outing on his Facebook profile page. So Alice clicked on the accompanying Web link, expecting to see Bob's photos. But the message had come from thieves who had hijacked Bob's Facebook account. And the link carried an infection. With a click of her mouse, Alice let the attackers usurp control of her Facebook account and company laptop. Later, they used Alice's company logon to slip deep inside the financial firm's network, where they roamed for weeks. They had managed to grab control of two servers, and were probing deeper, when they were detected.

Intrusions like this one can expose a company to theft of its most sensitive data. Such attacks illustrate a dramatic shift underway in the Internet underground. Cybercriminals are moving aggressively to take advantage of an unanticipated chink in corporate defenses: the use of social networks in workplace settings. They are taking tricks honed in the spamming world and adapting them to what's driving the growth of social networks: speed and openness of individuals communicating on the Internet.

What happened to Bob and Alice, the picnickers at the financial firm, illustrates how social networks help facilitate targeted attacks. As a rule, tech-security firms investigate breaches under non-disclosure agreements. Investigators increasingly find large botnets running inside corporate networks, where they can be particularly difficult to root out or disable. Social networks represent a vehicle to distribute malicious programs in ways that are not easily blocked.

Social networking attacks run the gamut. Earlier this year, one band of low-level cyberthieves, known in security circles as the Kneber gang, pilfered 68,000 account logons from 2,411 companies, including user names and passwords for 3,644 Facebook accounts. Active since late 2008, the Kneber gang has probably cracked into "a much higher number" of companies. Stolen credentials flow into eBay-like hacking forums where a batch of 1,000 Facebook user name and password pairs, guaranteed valid, sells for $75 to $200, depending on the number of friends tied to the accounts. On the high end, the Koobface worm, initially set loose several months ago, continues to increase in sophistication as it spreads through Facebook, Twitter, MySpace and other social networks. At its peak last August, more than 1 million Koobface-infected PCs inside North American companies were taking instructions from criminal controllers to carry out typical botnet criminal activities.

Social Networking Policies Still Scarce

Social networking is rapidly evolving into one of the biggest threats to data security out there today. But the reality is this medium is also a great way for your employees to collaborate and communicate. The challenge for many security professionals today lies in finding a balance between enabling the business while maintaining optimal security practices.

Most organizations do not have a social networking policy, despite giving employees unfettered access to the popular web sites, and according to a survey conducted by Symantec earlier this month. The survey was an attempt to gauge employee use of social media after a 2010 Symantec report on enterprise security found that enterprises view social media as a threat to security. In fact, eighty-four percent of CIOs and CISOs surveyed in

Symantec's 2010 *State of Enterprise Security Report*[6] considered social networking sites to be a serious threat to their security.

Approximately 50 percent of the 336 respondents to the survey said they access Facebook or YouTube at least once a day, with 16 percent indicating they access the sites between three and five times daily. More than half access the sites for business reasons, according to the research. Another 46 percent said the sites were accessed for personal reasons. In addition, 13 percent admit to circumventing company rules around social media. Among organizations who responded, 42 percent said their organization does not block employee access to social media sites, and has no policy in place around social media use. Only 5 percent indicated a complete blocking of the sites at work, a solution that is not really feasible in today's business environment.

Most companies will need to allow employee access to social networking sites, both for business reasons and because employees have begun to demand it. In fact, 32 percent of survey respondents indicated that being banned from social networks on the job would play a role in their decision to work for an organization.

Basic Security Measures

If you are using social networks and wish to minimize your personal security risk when doing so, you should follow some basic security tips. Symantec offers seven tips for users of a social network who want to protect their personal information. Topping this list is to (i) never share the password used to enter the site. Not even a best friend or spouse is a safe haven. Users of Facebook and other social networks should also be aware of the "digital crumbs" they leave behind. Photos, videos and comments posted on the Web are often there forever, so (ii) never post anything you wouldn't want the public, your neighbor or future employer to see. Also, (iii) never post sensitive information, such as a phone number, e-mail or birthday; and there's no need to share status updates, such as, "Off to Vegas for the weekend". Such information could be useful to criminals in your town.

Thirdly, we advise social network users to (iv) ignore links, supposedly sent from friends that have enticing titles like, "Check Out The Best Beach Bods." Chances are the link came from a hacker who broke into a friend's account. Another tip is to (v) make sure links posted to a Facebook wall are safe. While Symantec suggest the use of its Norton Safe Web software, other security vendors offer similar products. Such applications scan for links that take people to sites built by hackers to steal personal information. We also encourage people to (vi) limit their "circle of trust" on social networking sites to family and friends. Ignore requests from people you do not know, it could be a cyber-criminal. Finally, people need to (vii) stay informed of Facebook or other social networks privacy settings, which change often. In the last five years, Facebook's privacy policy has grown from about 1,000 words to today's 5,830 words.

Social Networking Rules of Engagement

Symantec encourages some basic rules to follow when engaging in social networks:

- **Don't post too much information** that could identify you or your location, including your last name, your school or business, where you live, where you spend time, your phone number or email address.

[6] The 2010 State of Enterprise Security report is based on input from 2100 enterprises around the world. The report finds that security IT's top concern as organizations experience frequent and increasingly effective cyber attacks. The costs of these attacks is high, and enterprise security is becoming more difficult. Symantec provides key security strategies to help security IT cope with this challenging landscape.

.

- **Use your site's privacy features** to limit personal posts to people you know and trust. Don't add people to your trusted list unless you know exactly who they are. Remove "friends" who post mean or untrue comments, or information that compromises your security.

- **Don't meet people you don't know**. Unless you can confirm exactly who they are, never agree to meet online friends in person. And even if you can confirm their identity, take precautions by meeting in a public, group setting.

- **Don't post suggestive pictures** or images that might give strangers clues about your identity or location. These pictures compromise your security, and they may affect how relatives, future employers, and even college admissions counselors perceive you.

- **Monitor your blog** for compromising information your friends may have added. Delete anything you don't want people to see, and consider removing offending posters from your friend list.

- **Don't lie about your age**. Acting older than you are can put you in dangerous situations. If you don't meet the age requirement, look for sites like Live Journal™, which offer lower age requirements and a safer environment.

- **Don't ever provide financial information** online without first checking with your parents, even on Web sites that appear to be legitimate. They may be fake or "phising" Web sites that exist only to steal your information.

- **What you say on a social networking site may become public** even if you post it in a private area. Don't use your account to spread rumors or disclose personal information about others. Your actions could have serious implications for you and your parents.

Conclusions

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention by governments worldwide. Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk online as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security.

Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal. The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Web pages such as the e-commerce sites sometimes hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes can also sometimes fall between the cracks.

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes. Clearly, law enforcement is fighting increasingly sophisticated and organized threats; therefore, it continues to need additional resources — funding for skilled personnel and cutting-edge technology — to expand its capabilities.

Policy Recommendations

Symantec asks the Committee, as you consider new cyber crime legislation in the area of social networking or other information security issues, to take under consideration the following recommendations:

Focus on the behavior, not technology. When considering new cybercrime laws focus on a behavioral approach to public policy that focuses on punishing bad behavior versus regulating the technology. For example, laws should criminalize the act of intentionally accessing a computer without authorization, or intentionally obtaining or transmitting personal information with the intent of injuring or defrauding a person or damaging a computer, not simply outlaw programs capable of collecting or transmitting data. Those programs, like other technologies, may have many legitimate uses outside the hands of a criminal. Another example of a behavioral approach would be to criminalize activity to intentionally impair the security protections of a computer.

Increase cybercrime penalties. Stronger penalties are needed to punish and deter bad actors who seek to capture information from a user's computer without authorization. It is unconscionable that cyber crime is going unpunished to the degree that it is around the world and governments worldwide must come to grips with the escalating threats. We fully support strengthening enforcement measures to go after these increasingly emboldened bad actors. Of course, penalties in criminal law must also account for innocent, unsuspecting users whose computers are unknowingly taken over by cyber criminals and used as a platform to orchestrate cyber crime on other users' computers -- often the case in botnet herding.

Develop a model approach for use globally. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber crime will be complicated. A globally harmonized framework of legislation against e-crime is needed. Governments around the work need to agree on the definitions of e-crime and of phishing so that attackers from all jurisdictions can be aggressively pursued in the criminal justice system. Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber crime havens.

Build a strong federal law enforcement and private industry partnership. Federal law enforcement needs to continue to build a strong partnership with State and local law enforcement by which we share expertise, equipment, and avoid costly duplication and fragmentation. Federal law enforcement should work in partnership with industry to address cybercrime and security. This should not be a top down approach through excessive government regulation or mandates. Rather, we need a true partnership where we can discuss challenges and develop effective solutions that do not pose a threat to individual privacy. Federal law enforcement can also take more of a leadership role in developing the means of educating our young people concerning the responsible use of the Internet.

Enact a comprehensive federal data security and breach notice law. Symantec strongly urges the enactment of a strong, federally pre-emptive national data security and breach law. While poor data security or failure to notify in the event of a breach is not itself cyber crime, common sense security and breach notice are perhaps the most important prophylactic measures that could be taken to reduce the volume of future cyber crime. In particular, we support the establishment of a presumption that there is no significant risk of harm associated with data that has been encrypted or otherwise rendered unusable or indecipherable. This is a clear incentive for businesses to adopt proven security as a roadmap to compliance that will make a real difference in reducing cyber crime. Further, we strongly support the safe harbor for nationally and internationally recognized industry standards, such as the PCI standards and related ISO standards. These two key provisions – the safe harbor for encryption and the safe harbor for adopting widely accepted industry standards – give companies that want to help protect their customers a critically needed roadmap for compliance when protecting electronic data.

* * * *

Mr. Chairman and Members of the Committee, Symantec appreciates the opportunity to provide its input on cybercrime. We share the Committee's goals to ensure that we have a robust and effective long-term strategy for combating cybercrime on social networks, protecting our nation's critical infrastructure, enhancing information security and protecting privacy so the Internet reaches its full potential for expanding communications, facilitating commerce, and bringing countless other benefits to our society. Symantec looks forward to continuing to work with the Committee as it considers cybercrime legislation in this area. Thank you.